



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,536	08/03/2001	John R. McGarvey	5577-236	6803
58505 7590 11/09/2007 STEVENS & SHOWALTER, L.L.P. BOX IBM 7019 CORPORATE WAY DAYTON, OH 45459-4238			EXAMINER HENNING, MATTHEW T	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 11/09/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/921,536

Applicant(s)

MCGARVEY ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 9/4/2007.

2 **DETAILED ACTION**

3 *Response to Arguments*

4 Applicant's arguments filed 9/4/2007 have been fully considered but they are not
5 persuasive.

6 Regarding applicants' argument that neither Bartolomeos nor Kaliski teach a common
7 nonce associated with each of a plurality of servers from an entity other than the client or the
8 servers, the examiner does not find the argument persuasive for the reasons presented below.

9 First, in response to applicant's arguments against the references individually, one cannot
10 show nonobviousness by attacking references individually where the rejections are based on
11 combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re*
12 *Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the applicants argue
13 each of Bartolomeos and Kaliski individually, but fail to address what the combination of the
14 teachings of these references would have suggested to the ordinary person of skill and creativity
15 in the art at the time of invention.

16 Regarding applicants' argument that Kaliski fails to teach a common nonce being
17 obtained from an entity other than the plurality of servers or the client, the examiner does not
18 find the argument persuasive. Kaliski has not been relied upon as solely teaching this limitation.
19 Rather, Kaliski teaches that the client can sign a message which contains a nonce for each server,
20 wherein each nonce is received from its respective server, then nonces are placed into a single
21 message at the client, which is then signed by the client. This can be seen in Kaliski Paragraphs
22 0083-0085. It is the teachings of Bartolomeos which have been relied upon as teaching that a

Art Unit: 2131

1 single server (middle tier server) provides the request for authentication data to the client for a
2 multiplicity of servers, as can be seen on Page 13 Lines 9-11 and Line 24 - Page 14 Line 6.
3 These teachings would suggest to the ordinary person skilled in the art that when employing the
4 teachings of Kaliski in the authentication system of Bartolomeos, the nonces would be collected
5 at a single server, and then transmitted in a single authentication request to the client. As such,
6 the examiner does not find the argument persuasive.

7 Regarding applicants' argument that Kaliski does not teach a common nonce, but rather
8 teaches independent nonces, the examiner does not find the argument persuasive. Each server's
9 nonce, in Kaliski, is equivalent to the "nonce contributions" of the instant application. That is,
10 each server's nonce is collected into a single message, as shown in Paragraph 0085 of Kaliski,
11 and this message is signed. It is the message that is equivalent to the common nonce of the
12 instant application. Therefore, the examiner does not find the argument persuasive.

13 Regarding applicants' argument that in Kaliski the client generates separate different
14 messages, each containing a different signed nonce, and each being sent only to its respective
15 server, the examiner does not find the argument persuasive. The applicants appear to have
16 misread and/or misinterpreted the teachings of Kaliski. Clearly, in paragraph 0085, Kaliski
17 teaches that "the recovery client 220 can generate 650 proof data by digitally signing **a message**
18 containing **the various nonces**".⁴ Kaliski further goes on to teach that each server verifies that
19 its corresponding nonce was included in the signed message. Clearly, this teaches a common
20 nonce, the message containing the various nonces, being signed and sent to the plurality of
21 servers. As such, the examiner does not find the argument persuasive.

1 Regarding applicants' argument that in Kaliski, if the individual nonces were each sent to
2 a middle tier server, the essence of the invention would be usurped, the examiner does not find
3 the argument persuasive. This mere allegation is unsupported by any evidence. Nowhere does
4 Kaliski teach that the nonces must be transmitted directly from the client to the server, and one of
5 ordinary skill in the art would not come away with this conclusion upon reading Kaliski.
6 Furthermore, the portion of Kaliski (the security of the strong secret data K) which the applicants
7 argue would be ruined by collection of the nonces at a middle tier server, would not be
8 jeopardized by collecting nonces at a middle tier server because the nonces are used for
9 authenticating the client to the server, not for gaining access to the secret data.

10 Even further still, Bartolomeos is not concerned with the storage and protection of strong
11 secret data K, but rather is concerned with authenticating the user of a client machine. Kaliski
12 teaches a method of doing so using server nonces which are combined into a single message
13 which is signed using the users private key, of a public/private key pair. In modifying the
14 authentication system of Bartolomeos by the teachings of Kaliski, one of ordinary skill in the art
15 would not find reason to include the teachings of Kaliski which regard the strong secret data, as
16 this is not part of the authentication teachings of Kaliski. As such, the examiner does not find the
17 argument persuasive.

18 Regarding applicants' argument that "each nonce" of Kaliski does not authenticate the
19 client to the plurality of servers, the examiner does not find the argument persuasive. Again, the
20 applicants have mischaracterized the reference and the rejection. The examiner points out that in
21 the rejection, each nonce as taught by Kaliski is equivalent to a pre-nonce contribution of the
22 instant invention, while the message containing the nonces as taught by Kaliski is equivalent to

Art Unit: 2131

1 the common nonce of the instant invention. It is the message containing the nonces which is
2 signed by the client in order to provide authentication of the user to each of the servers. As such,
3 the examiner does not find the argument persuasive.

4 Because the examiner has not found the arguments persuasive, the examiner has
5 maintained the previously presented prior art rejections.

6 All objections and rejections not set forth below have been withdrawn.

7 Claims 1-32 have been examined.

8
9 ***Claim Rejections - 35 USC § 103***

10 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
11 obviousness rejections set forth in this Office action:

12 *A patent may not be obtained though the invention is not identically disclosed or*
13 *described as set forth in section 102 of this title, if the differences between the subject matter*
14 *sought to be patented and the prior art are such that the subject matter as a whole would have*
15 *been obvious at the time the invention was made to a person having ordinary skill in the art to*
16 *which said subject matter pertains. Patentability shall not be negated by the manner in which*
17 *the invention was made.*
18

19 Claims 1-3, 5, 7-11, 14-15, and 26-32 are rejected under 35 U.S.C. 103(a) as being
20 unpatentable over Bartolomeos et al. (WO 99/56194) hereinafter referred to as Bartolomeos, and
21 further in view of Kaliski, JR. (Patent Application Publication 2001/0055388) hereinafter
22 referred to as Kaliski.

23 Regarding claim 1, Bartolomeos disclosed a method for a middle-tier server (See
24 Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element 110(I)) to a
25 plurality of servers (See Bartolomeos Servers 120(2)-120(M)), the method comprising:

Art Unit: 2131

1 providing a request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11);
2 receiving the authentication data at the middle-tier server (See Bartolomeos Page 13 Lines 9-11);
3 and providing authentication data to the plurality of servers to authenticate the client to the
4 plurality of servers (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos failed
5 to disclose that the authentication data was a common nonce associated with the plurality of
6 servers, or that the common nonce was signed by the client prior to being used to authenticate the
7 client. However, Bartolomeos did suggest that any type of authentication could have been used,
8 and that the disclosed username and password were simply one embodiment (See Bartolomeos
9 Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to
10 request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

11 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
12 message with the clients private key, the message containing a nonce from each of the servers,
13 and the private key being of a public/private key pair. Kaliski further teaches that the signed
14 message is returned to server, wherein the client is authenticated if the server verifies the
15 signature of the message, as well as verifying that the message contains its corresponding nonce
16 (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos
19 by having each server provide a nonce for the client, having the client sign a message containing
20 the nonces, having the client return the signed message to server 120(1), authenticating the client
21 using the message, and if authenticated, providing the signed message to each of servers 120(2)-
22 120(M) which then use the signed message to authenticate the client. This would have been

Art Unit: 2131

1 obvious because the ordinary person skilled in the art would have been motivated to provide a
2 more secure authentication than User ID and Password, and further would have been motivated
3 to ensure that the authentication data is fresh and not a replay of previous authentication data.

4 In this combination, it further would have been obvious to the ordinary person skilled in
5 the art at the time of invention for Server 120(1) to have collected the nonces from Servers
6 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.
7 This would have been obvious because Bartolomeos disclosed only server 120(1) requesting
8 authentication data from the client, and furthermore Bartolomeos is concerned with eliminating
9 repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have
10 recognized that sending an individual nonce message for each of the M servers would have been
11 repetitive, tedious, and burdensome. Furthermore, sending one message containing all the
12 nonces to the client would have been obvious because the ordinary person skilled in the art
13 would have been motivated to eliminate unnecessary traffic through network 110.

14 Regarding claim 26, Bartolomeos disclosed a system for a middle-tier server (See
15 Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element 110(I)) to a
16 plurality of servers (See Bartolomeos Servers 120(2)-120(M)), comprising: means for providing
17 a request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11); means for
18 receiving the authentication data at the middle-tier server (See Bartolomeos Page 13 Lines 9-11);
19 and means for providing authentication data to the plurality of servers to authenticate the client
20 to the plurality of servers (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos
21 failed to disclose that the authentication data was a common nonce associated with the plurality
22 of servers, or that the common nonce was signed by the client prior to being used to authenticate

1 the client. However, Bartolomeos did suggest that any type of authentication could have been
2 used, and that the disclosed username and password were simply one embodiment (See
3 Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting
4 the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

5 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
6 message with the clients private key, the message containing a nonce from each of the servers,
7 and the private key being of a public/private key pair. Kaliski further teaches that the signed
8 message is returned to server, wherein the client is authenticated if the server verifies the
9 signature of the message, as well as verifying that the message contains its corresponding nonce
10 (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

11 It would have been obvious to the ordinary person skilled in the art at the time of
12 invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos
13 by having each server provide a nonce for the client, having the client sign a message containing
14 the nonces, having the client return the signed message to server 120(1), authenticating the client
15 using the message, and if authenticated, providing the signed message to each of servers 120(2)-
16 120(M) which then use the signed message to authenticate the client. This would have been
17 obvious because the ordinary person skilled in the art would have been motivated to provide a
18 more secure authentication than User ID and Password, and further would have been motivated
19 to ensure that the authentication data is fresh and not a replay of previous authentication data.

20 In this combination, it further would have been obvious to the ordinary person skilled in
21 the art at the time of invention for Server 120(1) to have collected the nonces from Servers
22 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.

Art Unit: 2131

1 This would have been obvious because Bartolomeos disclosed only server 120(1) requesting
2 authentication data from the client, and furthermore Bartolomeos is concerned with eliminating
3 repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have
4 recognized that sending an individual nonce message for each of the M servers would have been
5 repetitive, tedious, and burdensome. Furthermore, sending one message containing all the
6 nonces to the client would have been obvious because the ordinary person skilled in the art
7 would have been motivated to eliminate unnecessary traffic through network 110.

8 Regarding claim 27, Bartolomeos a computer program product for a middle-tier server
9 (See Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element
10 110(I)) to a plurality of servers (See Bartolomeos Servers 120(2)-120(M)), comprising: a
11 computer readable media having computer readable program code embodied therein, the
12 computer readable program code comprising: computer readable program code that provides a
13 request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11); computer
14 readable program code that receives the authentication data at the middle-tier server (See
15 Bartolomeos Page 13 Lines 9-11); and computer program readable code that provides
16 authentication data to the plurality of servers to authenticate the client to the plurality of servers
17 (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos failed to disclose that the
18 authentication data was a common nonce associated with the plurality of servers, or that the
19 common nonce was signed by the client prior to being used to authenticate the client. However,
20 Bartolomeos did suggest that any type of authentication could have been used, and that the
21 disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines

Art Unit: 2131

1 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the
2 client's authentication data (See Bartolomeos Page 13 Lines 9-11).

3 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
4 message with the clients private key, the message containing a nonce from each of the servers,
5 and the private key being of a public/private key pair. Kaliski further teaches that the signed
6 message is returned to server, wherein the client is authenticated if the server verifies the
7 signature of the message, as well as verifying that the message contains its corresponding nonce
8 (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

9 It would have been obvious to the ordinary person skilled in the art at the time of
10 invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos
11 by having each server provide a nonce for the client, having the client sign a message containing
12 the nonces, having the client return the signed message to server 120(1), authenticating the client
13 using the message, and if authenticated, providing the signed message to each of servers 120(2)-
14 120(M) which then use the signed message to authenticate the client. This would have been
15 obvious because the ordinary person skilled in the art would have been motivated to provide a
16 more secure authentication than User ID and Password, and further would have been motivated
17 to ensure that the authentication data is fresh and not a replay of previous authentication data.

18 In this combination, it further would have been obvious to the ordinary person skilled in
19 the art at the time of invention for Server 120(1) to have collected the nonces from Servers
20 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.
21 This would have been obvious because Bartolomeos disclosed only server 120(1) requesting
22 authentication data from the client, and furthermore Bartolomeos is concerned with eliminating

Art Unit: 2131

1 repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have
2 recognized that sending an individual nonce message for each of the M servers would have been
3 repetitive, tedious, and burdensome. Furthermore, sending one message containing all the
4 nonces to the client would have been obvious because the ordinary person skilled in the art
5 would have been motivated to eliminate unnecessary traffic through network 110.

6 Regarding claim 28, Bartolomeos disclosed a method of authenticating a client (See
7 Bartolomeos Fig. 1 Element 100(I)), comprising: receiving at a server (See Bartolomeos Fig. 1
8 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements 120(2)-120(M)),
9 authentication data that is provided to each of the plurality of servers (See Bartolomeos Page 14
10 Lines 1-4) from an entity other than the client or the plurality of servers (See Bartolomeos Page
11 14 Lines 1-4 server 120(1)), the authentication data being associated with each of the plurality of
12 servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11); and authenticating the
13 client based on the received authentication data (See Bartolomeos Page 14 Lines 5-6), but
14 Bartolomeos failed to disclose that the authentication data was a common nonce associated with
15 the plurality of servers, or that the common nonce was signed by the client prior to being used to
16 authenticate the client. However, Bartolomeos did suggest that any type of authentication could
17 have been used, and that the disclosed username and password were simply one embodiment
18 (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1)
19 contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines
20 9-11).

21 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
22 message with the clients private key, the message containing a nonce from each of the servers,

1 and the private key being of a public/private key pair. Kaliski further teaches that the signed
2 message is returned to server, wherein the client is authenticated if the server verifies the
3 signature of the message, as well as verifying that the message contains its corresponding nonce
4 (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

5 It would have been obvious to the ordinary person skilled in the art at the time of
6 invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos
7 by having each server provide a nonce for the client, having the client sign a message containing
8 the nonces, having the client return the signed message to server 120(1), authenticating the client
9 using the message, and if authenticated, providing the signed message to each of servers 120(2)-
10 120(M) which then use the signed message to authenticate the client. This would have been
11 obvious because the ordinary person skilled in the art would have been motivated to provide a
12 more secure authentication than User ID and Password, and further would have been motivated
13 to ensure that the authentication data is fresh and not a replay of previous authentication data.

14 In this combination, it further would have been obvious to the ordinary person skilled in
15 the art at the time of invention for Server 120(1) to have collected the nonces from Servers
16 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.
17 This would have been obvious because Bartolomeos disclosed only server 120(1) requesting
18 authentication data from the client, and furthermore Bartolomeos is concerned with eliminating
19 repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have
20 recognized that sending an individual nonce message for each of the M servers would have been
21 repetitive, tedious, and burdensome. Furthermore, sending one message containing all the

Art Unit: 2131

1 nonces to the client would have been obvious because the ordinary person skilled in the art
2 would have been motivated to eliminate unnecessary traffic through network 110.

3 Regarding claim 31, Bartolomeos disclosed a system for authenticating a client (See
4 Bartolomeos Fig. 1 Element 100(I)), comprising: means for receiving at a server (See
5 Bartolomeos Fig. 1 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements
6 120(2)-120(M)), authentication data that is provided to each of the plurality of servers (See
7 Bartolomeos Page 14 Lines 1-4) from an entity other than the client or the plurality of servers
8 (See Bartolomeos Page 14 Lines 1-4 server 120(1)), the authentication data being associated with
9 each of the plurality of servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11);
10 and means for authenticating the client based on the received authentication data (See
11 Bartolomeos Page 14 Lines 5-6), but Bartolomeos failed to disclose that the authentication data
12 was a common nonce associated with the plurality of servers, or that the common nonce was
13 signed by the client prior to being used to authenticate the client. However, Bartolomeos did
14 suggest that any type of authentication could have been used, and that the disclosed username
15 and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and
16 Bartolomeos did disclose only server 120(1) contacting the client to request the client's
17 authentication data (See Bartolomeos Page 13 Lines 9-11).

18 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
19 message with the clients private key, the message containing a nonce from each of the servers,
20 and the private key being of a public/private key pair. Kaliski further teaches that the signed
21 message is returned to server, wherein the client is authenticated if the server verifies the

Art Unit: 2131

signature of the message, as well as verifying that the message contains its corresponding nonce
(See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

1 Regarding claim 32, Bartolomeos disclosed a computer program product for
2 authenticating a client (See Bartolomeos Fig. 1 Element 100(I)), comprising: a computer
3 readable media having computer program code embodied therein, the computer readable
4 program code comprising: computer readable program code which receives at a server (See
5 Bartolomeos Fig. 1 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements
6 120(2)-120(M)), authentication data that is provided to each of the plurality of servers (See
7 Bartolomeos Page 14 Lines 1-4) from an entity other than the client or the plurality of servers
8 (See Bartolomeos Page 14 Lines 1-4 server 120(1)), the authentication data being associated with
9 each of the plurality of servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11);
10 and computer readable program code which authenticates the client based on the received
11 authentication data (See Bartolomeos Page 14 Lines 5-6), but Bartolomeos failed to disclose that
12 the authentication data was a common nonce associated with the plurality of servers, or that the
13 common nonce was signed by the client prior to being used to authenticate the client. However,
14 Bartolomeos did suggest that any type of authentication could have been used, and that the
15 disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines
16 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the
17 client's authentication data (See Bartolomeos Page 13 Lines 9-11).

18 Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a
19 message with the clients private key, the message containing a nonce from each of the servers,
20 and the private key being of a public/private key pair. Kaliski further teaches that the signed
21 message is returned to server, wherein the client is authenticated if the server verifies the

Art Unit: 2131

1 signature of the message, as well as verifying that the message contains its corresponding nonce
2 (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

3 It would have been obvious to the ordinary person skilled in the art at the time of
4 invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos
5 by having each server provide a nonce for the client, having the client sign a message containing
6 the nonces, having the client return the signed message to server 120(1), authenticating the client
7 using the message, and if authenticated, providing the signed message to each of servers 120(2)-
8 120(M) which then use the signed message to authenticate the client. This would have been
9 obvious because the ordinary person skilled in the art would have been motivated to provide a
10 more secure authentication than User ID and Password, and further would have been motivated
11 to ensure that the authentication data is fresh and not a replay of previous authentication data.

12 In this combination, it further would have been obvious to the ordinary person skilled in
13 the art at the time of invention for Server 120(1) to have collected the nonces from Servers
14 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.
15 This would have been obvious because Bartolomeos disclosed only server 120(1) requesting
16 authentication data from the client, and furthermore Bartolomeos is concerned with eliminating
17 repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have
18 recognized that sending an individual nonce message for each of the M servers would have been
19 repetitive, tedious, and burdensome. Furthermore, sending one message containing all the
20 nonces to the client would have been obvious because the ordinary person skilled in the art
21 would have been motivated to eliminate unnecessary traffic through network 110.

1 Regarding claim 2, the combination of Bartolomeos and Kaliski disclosed that the step of
2 obtaining a common nonce comprises the step of generating, by an entity other than the client
3 (110(1)) or the plurality of servers (120(2)-120(M)), a common nonce based on information
4 obtained from each of the plurality of servers (See Kaliski Paragraphs 0083-0086 as well as the
5 rejection of claim 1 above, wherein server 120(1) generates the message).

6 Regarding claim 3, the combination of Bartolomeos and Kaliski disclosed that the step of
7 generating a common nonce comprises the steps of: obtaining pre-nonce contributions from the
8 plurality of servers (See Kaliski Paragraphs 0083-0086); combining the pre-nonce contributions
9 to provide a single pre-nonce token (See Kaliski Paragraph 0085 and the rejection of claim 1
10 above); and providing the common nonce based on the pre-nonce token (See the rejection of
11 claim 1 above).

12 Regarding claim 5, the combination of Bartolomeos and Kaliski disclosed that the step of
13 combining the pre-nonce contributions to provide a single pre-nonce token comprises
14 concatenating the pre-nonce contributions (See Kaliski Paragraph 0085 and the rejection of claim
15 1 above).

16 Regarding claim 7, the combination of Bartolomeos and Kaliski disclosed that the step of
17 obtaining pre-nonce contributions comprises the steps of requesting a pre-nonce contribution
18 from each of the plurality of servers and receiving the pre-nonce contributions from the plurality
19 of servers (See Kaliski Paragraph 0083 and the rejection of claim 1 above).

20 Regarding claims 8-10, the combination of Bartolomeos and Kaliski disclosed that
21 requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of
22 servers (See Kaliski paragraph 0083 and the rejection of claim 1 above); wherein the

Art Unit: 2131

1 authenticated requests are encrypted, and include a source of the request (wherein it was well
2 known in the art of information security at the time of invention to use authenticated requests, to
3 encrypt communications, and to include the source of a message with the message).

4 Regarding claim 11, the combination of Bartolomeos and Kaliski disclosed that the pre-
5 nonce contributions include at least one of an identification of a server of the plurality of servers
6 and a random number (See Kaliski Paragraphs 0083-0086).

7 Regarding claim 14, the combination of Bartolomeos and Kaliski disclosed receiving a
8 transaction identification from a trusted server of the plurality of servers and associating the
9 transaction identification with the common nonce (See Kaliski Paragraph 0085 and the rejection
10 of claim 1 above).

11 Regarding claim 15, the combination of Bartolomeos and Kaliski disclosed tracking use
12 of the common nonce based on the transaction identification (See Kaliski Paragraph 0085 and
13 the rejection of claim 1 above).

14 Regarding claim 29, the combination of Bartolomeos and Kaliski disclosed that the
15 common nonce is provided by a trusted third party (See the rejection of claim 28 above, wherein
16 the common nonce is provided by the server 120(1)).

17 Regarding claim 30, the combination of Bartolomeos and Kaliski disclosed that the
18 common nonce is generated by an entity other than the client or the plurality of servers based on
19 information provided by each of the plurality of servers (See the rejection of claim 28 above).

20 Claims 4, 6, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over
21 the combination of Bartolomeos and Kaliski as applied to claim 3 above, and further in view of
22 Schneier (Applied Cryptography).

1 Regarding claim 4, the combination of Bartolomeos and Kaliski disclosed providing a
2 common nonce (See Kaliski Paragraph 0085 and the rejection of claim 1 above), but failed to
3 disclose reducing the nonce challenges to provide the common nonce. However, the
4 combination of Bartolomeos and Kaliski did disclose digitally signing a message containing the
5 nonce challenges (See the rejection of claim 1 above).

6 Schneier teaches that when digitally signing a message, it is practical to hash the message
7 and encrypt the hash, with a private key, as the signature, rather than encrypting the whole
8 message (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and
9 One-Way Hash Functions). Schneier also teaches that in such a system, to verify the signature,
10 the verifier hashes the message, decrypts the signed hash with the signers public key, and verifies
11 that the two hashes are the same (See Schneier Page 38 Section Signing Documents with Public-
12 Key Cryptography and One-Way Hash Functions).

13 It would have been obvious to the ordinary person skilled in the art at the time of
14 invention to employ the teachings of Schneier in the digital signatures of the combination of
15 Bartolomeos and Kaliski by providing a hash of the nonce message instead of the whole nonce
16 message for signing. This would have been obvious because the ordinary person skilled in the
17 art would have been motivated to increase the speed of the signing method, as well as reduce the
18 amount of data needing to be transmitted to the client.

19 Regarding claim 6, the combination of Bartolomeos, Kaliski, and Schneier disclosed that
20 the step of reducing the pre-nonce token to provide the common nonce comprises the step of
21 hashing the pre-nonce token utilizing a one-way hash function so as to provide the common
22 nonce (See the rejection of claim 4 above).

Art Unit: 2131

1 Regarding claim 20, the combination of Bartolomeos, Kaliski, and Schneier disclosed
2 that at least one of the plurality of servers carries out the steps of: receiving the signed common
3 nonce, the common nonce and the pre-nonce token; hashing the received pre-nonce token;
4 comparing the hashed pre-nonce token to the common nonce; indicating that the client is not
5 authenticated if the hashed pre-nonce token is different from the common nonce (See Kaliski
6 Paragraph 0085 and Schneier Page 38 Section Signing Documents with Public-Key
7 Cryptography and One-Way Hash Functions).

8 Regarding claims 12-13, the combination of Bartolomeos and Kaliski disclosed the client
9 checking the nonce challenge from the server for requisite strength, and aborting the
10 authentication process if the nonce challenge did not meet the requisite strength (See Kaliski
11 Paragraph 0084), but failed to disclose that this check included checking the signature of the
12 nonce challenge to verify that it was signed by the server.

13 Schneier teaches that digital signatures provide a means for verifying the sender of a
14 message (See Schneier Page 37 Signing Documents with Public Key Cryptography).

15 It would have been obvious to the ordinary person skilled in the art at the time of
16 invention to employ the teachings of Schneier in the nonce challenge system of Bartolomeos and
17 Kaliski by having the servers 120(2)-120(M) sign the challenges and having the server 120(1)
18 verify the signature of the challenges before using the challenges. This would have been obvious
19 because the ordinary person skilled in the art would have been motivated to protect against illicit
20 alteration of the challenge nonce.

Art Unit: 2131

1 Claims 16-19, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over
2 the combination of Bartolomeos and Kaliski as applied to claim 3 above, and further in view of
3 Menezes et al. (Handbook of Applied Cryptography).

4 Regarding claim 21, the combination of Bartolomeos and Kaliski disclosed the server
5 receiving the nonce challenges, and authenticating the client based on whether the nonce
6 challenges included the nonce challenge of the server (See Kaliski Paragraph 0085), but failed to
7 disclose that the nonce challenges included random numbers.

8 Menezes teaches that nonce challenges can be random numbers (See Menezes Page 398).

9 It would have been obvious to the ordinary person skilled in the art at the time of
10 invention to employ the teachings of Menezes in the nonce challenge system of the combination
11 of Bartolomeos and Kaliski by having the nonce challenges be random numbers. This would
12 have been obvious because the ordinary person skilled in the art would have been motivated to
13 provide uniqueness and timeliness assurances in the system in order to avoid replay and
14 interleaving attacks.

15 Regarding claims 16-17, and 22 the combination of Bartolomeos and Kaliski disclosed a
16 plurality of servers providing nonce challenges to a client in order to authenticate the client, and
17 verifying the nonce in the response to the challenge (See Kaliski Paragraphs 0083-0085) but
18 failed to disclose giving the nonce an expiration time and further authenticating the client based
19 on the expiration time.

20 Menezes teaches that when using nonce challenges the challenger should apply a timeout
21 period to the nonce and not authenticate the client if the response is received after the timeout
22 period has expired (See Menezes Page 398 Section (i)).

1 It would have been obvious to the ordinary person skilled in the art at the time of
2 invention to employ the teachings of Menezes in the nonce challenge system of the combination
3 of Bartolomeos and Kaliski by applying and checking a timeout period to the nonce when
4 authenticating a client. This would have been obvious because the ordinary person skilled in the
5 art would have been motivated to provide protection against replay and interleaving attacks.

6 Regarding claims 18-19, the combination of Bartolomeos and Kaliski disclosed using a
7 users public key to verify the signature of the nonce message by verifying that the signature
8 corresponded to the signature of the clients private/public key pair (See Kaliski Paragraph 0085),
9 but failed to disclose that the verifying server got the public key from a public key certificate and
10 also failed to disclose that the authentication would fail if the certificate was not trusted.

11 Menezes teaches that public key certificates are a means to store, distribute, and forward
12 public keys without danger of undetectable manipulation. Menezes also teaches that when using
13 a certificate for authentication, the certificate is received, the expiration date is checked, the
14 certification authority validity is checked, the signature of the certificate is checked, and the
15 certificate is checked to see if it has been revoked, and if these checks pass then the public key is
16 valid (See Menezes Pages 559-560).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Menezes in the authentication system of the combination of
19 Bartolomeos and Kaliski by obtaining the public key from a public key certificate and verifying
20 that the certificate is valid in order to use the public key to authenticate the client. This would
21 have been obvious because the ordinary person skilled in the art would have been motivated to
22 protect against undetected manipulation of the public key.

Art Unit: 2131

1 Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination
2 of Bartolomeos and Kaliski as applied to claim 1 above, and further in view of Day (US Patent
3 Number 6,052,784).

4 The combination of Bartolomeos and Kaliski disclosed a challenge nonce system (See
5 Kaliski Paragraphs 0083-0086) but failed to disclose the nonce being received from a trusted
6 third party and verifying the signature of the trusted third party.

7 Day teaches that a nonce can be signed by a trusted third party in order to authenticate the
8 nonce (See Day Col. 3 Paragraph 5).

9 It would have been obvious to the ordinary person skilled in the art at the time of
10 invention to employ the teachings of Day in the nonce challenge system of the combination of
11 Bartolomeos and Kaliski by having the nonce challenges signed by a certification authority prior
12 to sending the challenge to the client, and verifying the signature on the nonce. This would have
13 been obvious because the ordinary person skilled in the art would have been motivated to
14 prevent the nonce from being illicitly undetectably modified prior to the client receiving the
15 nonce challenge.

16 Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the
17 combination of Bartolomeos, Kaliski, and Day as applied to claim 23 above, and further in view
18 of Menezes.

19 The combination of Bartolomeos, Kaliski, and Day disclosed using a users public key to
20 verify the signature of the nonce message by verifying that the signature corresponded to the
21 signature of the clients private/public key pair (See Kaliski Paragraph 0085), but failed to

Art Unit: 2131

1 disclose that the verifying server got the public key from a public key certificate and also failed
2 to disclose that the authentication would fail if the certificate was not trusted.

3 Menezes teaches that public key certificates are a means to store, distribute, and forward
4 public keys without danger of undetectable manipulation. Menezes also teaches that when using
5 a certificate for authentication, the certificate is received, the expiration date is checked, the
6 certification authority validity is checked, the signature of the certificate is checked, and the
7 certificate is checked to see if it has been revoked, and if these checks pass then the public key is
8 valid (See Menezes Pages 559-560).

9 It would have been obvious to the ordinary person skilled in the art at the time of
10 invention to employ the teachings of Menezes in the authentication system of the combination of
11 Bartolomeos, Kaliski, and Day by obtaining the public key from a public key certificate and
12 verifying that the certificate is valid in order to use the public key to authenticate the client. This
13 would have been obvious because the ordinary person skilled in the art would have been
14 motivated to protect against undetected manipulation of the public key.

15 *Conclusion*

16 Claims 1-32 have been rejected.

17 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time
18 policy as set forth in 37 CFR 1.136(a).

19 A shortened statutory period for reply to this final action is set to expire THREE
20 MONTHS from the mailing date of this action. In the event a first reply is filed within TWO
21 MONTHS of the mailing date of this final action and the advisory action is not mailed until after
22 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2131


1 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
2 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
3 however, will the statutory period for reply expire later than SIX MONTHS from the mailing
4 date of this final action.

5 Any inquiry concerning this communication or earlier communications from the
6 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
7 The examiner can normally be reached on M-F 8-4.

8 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
9 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
10 organization where this application or proceeding is assigned is 571-273-8300.

11 Information regarding the status of an application may be obtained from the Patent
12 Application Information Retrieval (PAIR) system. Status information for published applications
13 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
14 applications is available through Private PAIR only. For more information about the PAIR
15 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
16 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
17 like assistance from a USPTO Customer Service Representative or access to the automated
18 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

19
20
21
22
23 /Matthew Henning/
24 Assistant Examiner
25 Art Unit 2131
26 11/6/2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100